National Cybersecurity Center of Excellence

Migration to Post-Quantum Cryptography Project

Update for the 4th PQC Standardization Conference

December 1, 2022

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

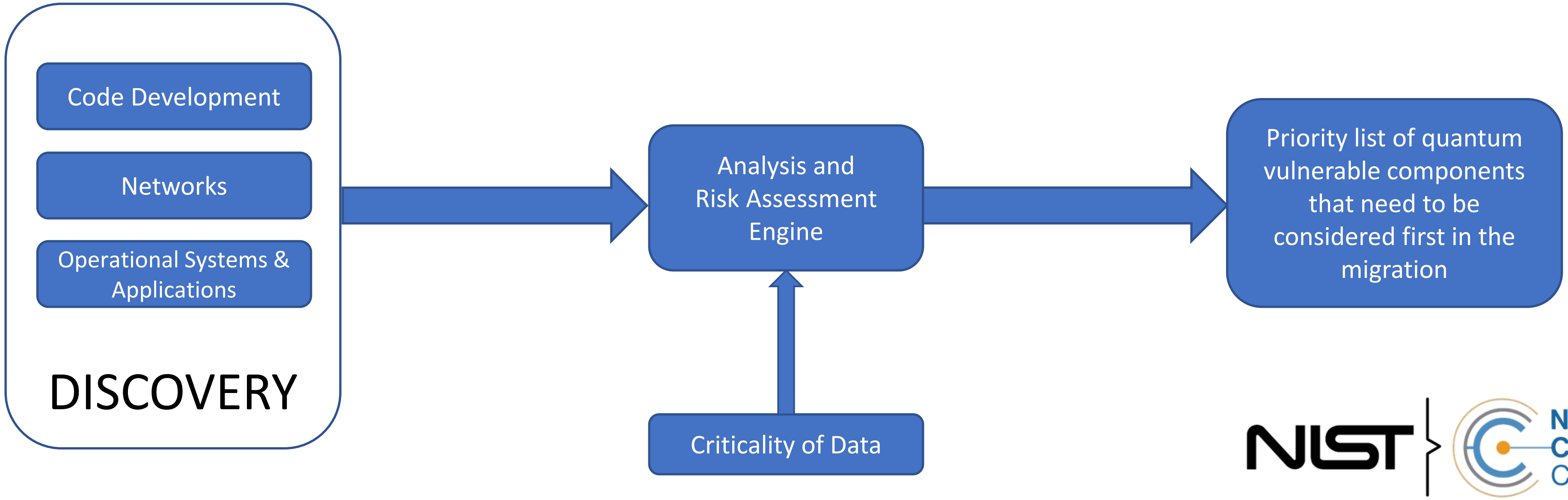
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCOE MIGRATION TO POST-QUANTUM CRYPTOGRAPHY PROJECT WORKSTREAMS

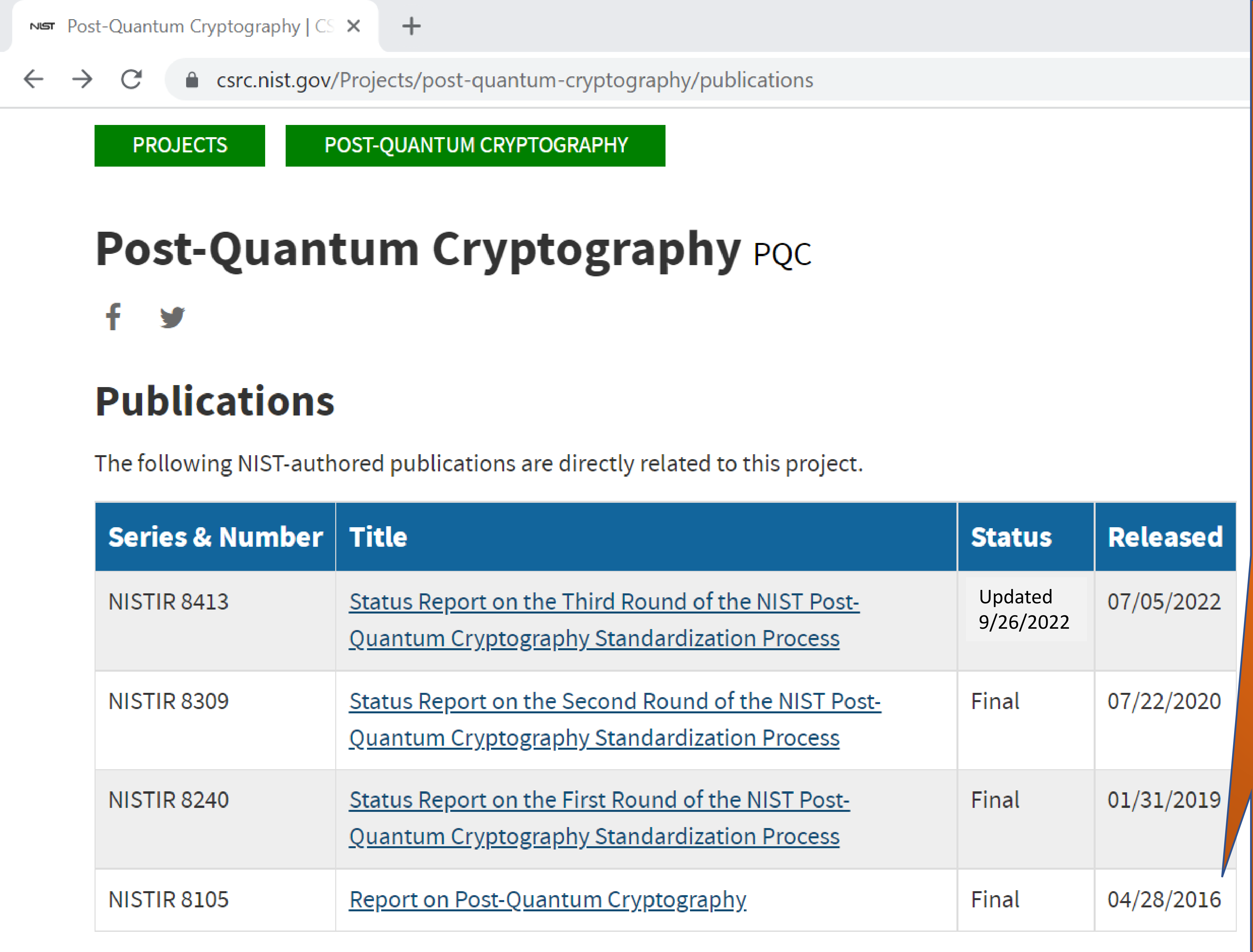
Workstream Name	Description
Quantum Vulnerable Algorithm Discovery	• Use discovery tools to detect and report the presence and use of quantum vulnerable cryptography with enough detail and context to inform risk analysis and remediation. • Standardize output formats
Interoperability	• Identifying the challenging problems and bottlenecks that one will face when implementing the first algorithms NIST will standardize as a result of the PQC Standardization Process in protocols such as TLS, SSH, MQTT, QUIC, and a standard like X.509.
Performance	• Identify • Metrics to measure (time, memory); • Protocols to test (e.g., TLS, SSH) and arch/devices to use; • Test conditions (network quality, deployment architectures) • For each test case, and for each implementing software component, measure performance of classical, PQC, and PQ-hybrid cases • Report on unique issues introduced by PQC algorithms • Propose and test solutions to the issues
Outreach / Standards	• Community Outreach
Lab Infrastructure	• Systems, services, and platforms to support technical builds

Discovery Workstream

Workstream Name	Description
Quantum Vulnerable Algorithm Discovery	• **Development Pipeline** - inspects code to find references to cryptography uses that are PQ vulnerable. • **Networks** - Network traffic PQ-vulnerable discovery • **Operational Systems and Applications** - Discovery of PQ-vulnerable applications and libraries at OS-level or provided by the OS itself. • **Risk Analysis** – Development, Network, and Operational Systems discovery informs risk assessment / identification of priorities for replacement


Code Development
Networks
Operational Systems & Applications
DISCOVERY
Analysis and Risk Assessment Engine
Criticality of Data
Priority list of quantum vulnerable components that need to be considered first in the migration

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE


NIST Post-Quantum Cryptography | CS
csrc.nist.gov/Projects/post-quantum-cryptography/publications
PROJECTS
POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography PQC

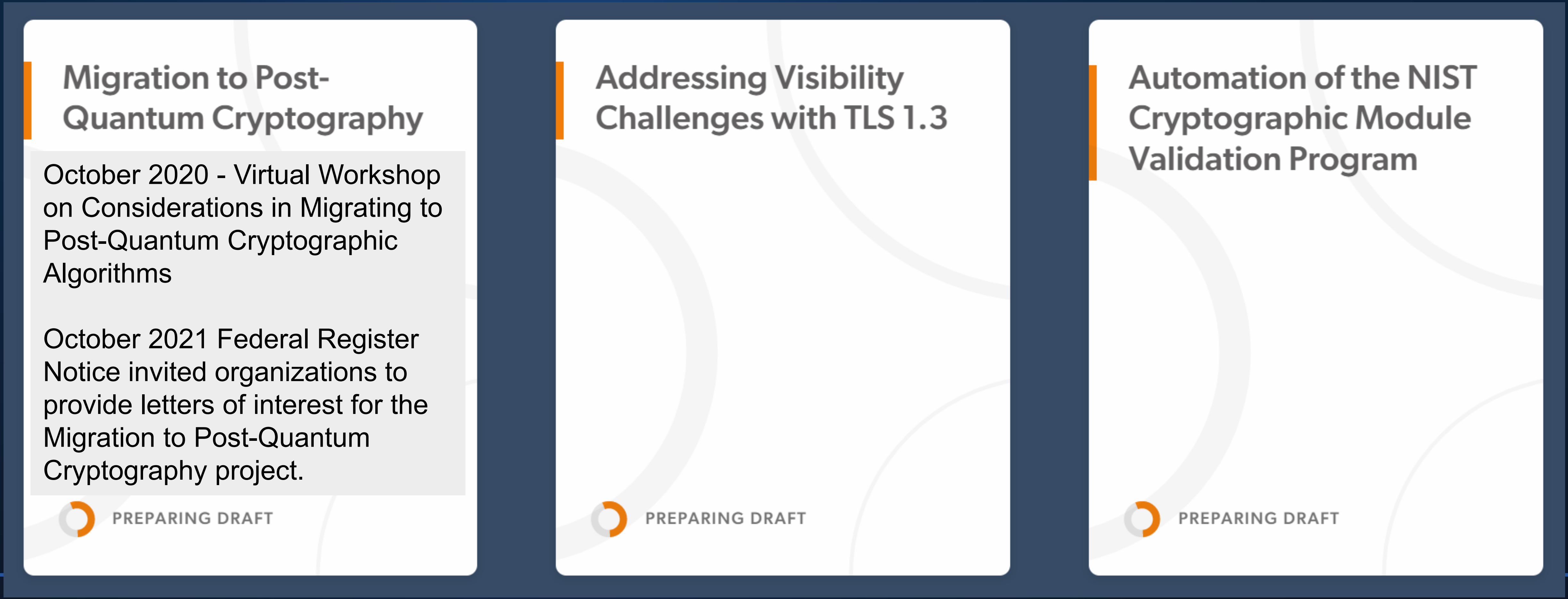
Publications

The following NIST-authored publications are directly related to this project.

Series & Number	Title	Status	Released
NISTIR 8413	Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process	Updated 9/26/2022	07/05/2022
NISTIR 8309	Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process	Final	07/22/2020
NISTIR 8240	Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process	Final	01/31/2019
NISTIR 8105	Report on Post-Quantum Cryptography	Final	04/28/2016

It has taken almost 20 years to deploy our modern public key cryptography infrastructure. It will take significant effort to ensure a smooth and secure migration from the current widely used cryptosystems to their quantum computing resistant counterparts. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing

NIST's National Cybersecurity Center of Excellence Applied Cryptography Projects



Migration to Post-Quantum Cryptography

October 2020 - Virtual Workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms

October 2021 Federal Register Notice invited organizations to provide letters of interest for the Migration to Post-Quantum Cryptography project.

PREPARING DRAFT

Addressing Visibility Challenges with TLS 1.3

PREPARING DRAFT

Automation of the NIST Cryptographic Module Validation Program

PREPARING DRAFT

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

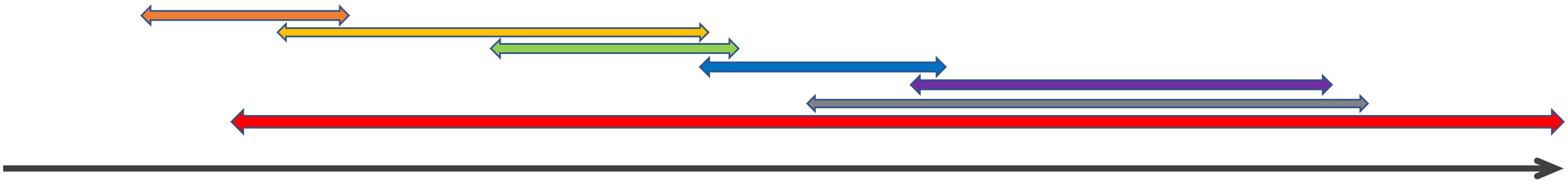
Goals of the NCCOE Migration to PQC Project

- Align and complement the NIST PQC standardization activities
- Develop practices to ease the migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to cryptanalytically relevant quantum computer (CRQC) attacks
- Deliver white papers, playbooks, and demonstrable implementations for organizations that provide cryptographic standards and protocols and enterprises that develop, acquire, implement, and service cryptographic products.

MIGRATION TO PQC PROJECT TIMELINE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

	DESCRIBE 〉	FORM TEAM 〉	DESIGN 〉	BUILD PLAN 〉	BUILD 〉	DOCUMENT 〉	OUTREACH 〉
Preliminary Research And Feasibility Discussion To Develop Initial Concept	Conduct workshop to scope the project and publish the description	Form the team, build the community of interest, and complete the Federal Register Notice, Letter of Interest, and CRADA	Design and engineer the architecture and usage scenarios taking into consideration resources	Develop the execution plan for building the demonstration based on the design	Compose, build the demonstration, and perform security functional tests	Develop the practice guide to publish as a public draft and final document	Present at public events and interact with community of interest



NCCOE Migration to PQC Project

- Audience: developers of products that use public-key cryptographic algorithms, integrators of such products, customer organizations that acquire or configure such products, and bodies that standardize protocols that employ or are dependent on public-key cryptographic algorithms.
- Demonstrate use of discovery tools to identify all instances of public-key algorithm use in an example network infrastructure's computer and communications hardware, operating systems, application programs, communications protocols, key infrastructures, and access control mechanisms.

NCCOE Migration to PQC Project

- Once the public-key cryptography components and associated assets in the enterprise are identified, the next element of the scope of the project is to prioritize those components that need to be considered first in the migration using a risk management methodology.
- provide systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across the different types of assets and supporting underlying technology

Migration to Post-Quantum Cryptography
Why Start Preparing Now?

The argument for starting now, to address the threat that a cryptanalytically relevant quantum computer (CRQC) will pose to existing security systems, is based on the following considerations:

a) cryptographic technologies are integrated into most of the digital products commonly used by organizations to run their daily operations;
b) some of the applications and systems used within energy, transportation, finance and government infrastructures have product lifetimes of 15 - 30 years, and even longer requirements for data protection and privacy;
c) fault-tolerant cryptographically relevant quantum computers, capable of breaking existing encryption algorithms and cryptographic systems (e.g., public-key infrastructures), are widely expected to be available within the above timeline;
d) the time needed to migrate installed cryptographic technologies (e.g., SHA1) to something newer can take many years;
e) the number of cryptographic systems that organizations will need to migrate to use new "quantum-safe" cryptography will be large; and
f) most organizations have no clear view of the cryptographic technologies used by their existing Information Management (IM), Information Technology (IT) and Operational Technology (OT) systems; this will make it difficult to discover and then prioritize the systems to be upgraded to post-quantum cryptography.

*Adapted from section 1.3 in the **Canadian National Quantum-Readiness BEST PRACTICES AND GUIDELINES** (Version 01 – July 7, 2021) authored by: Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)*

November 18, 2022 White House Memo
SUBJECT: Migrating to Post-Quantum Cryptography

- This memorandum describes preparatory steps for agencies to undertake as they begin their transition to PQC by conducting a prioritized inventory of cryptographic systems.
- Further, this memorandum provides transitional guidance to agencies in the period before PQC standards are finalized by the National Institute of Standards and Technology (NIST), after which OMB will issue further guidance.
- Within 30 days of the publication of this memorandum, agencies will designate a cryptographic inventory and migration lead for their organization.

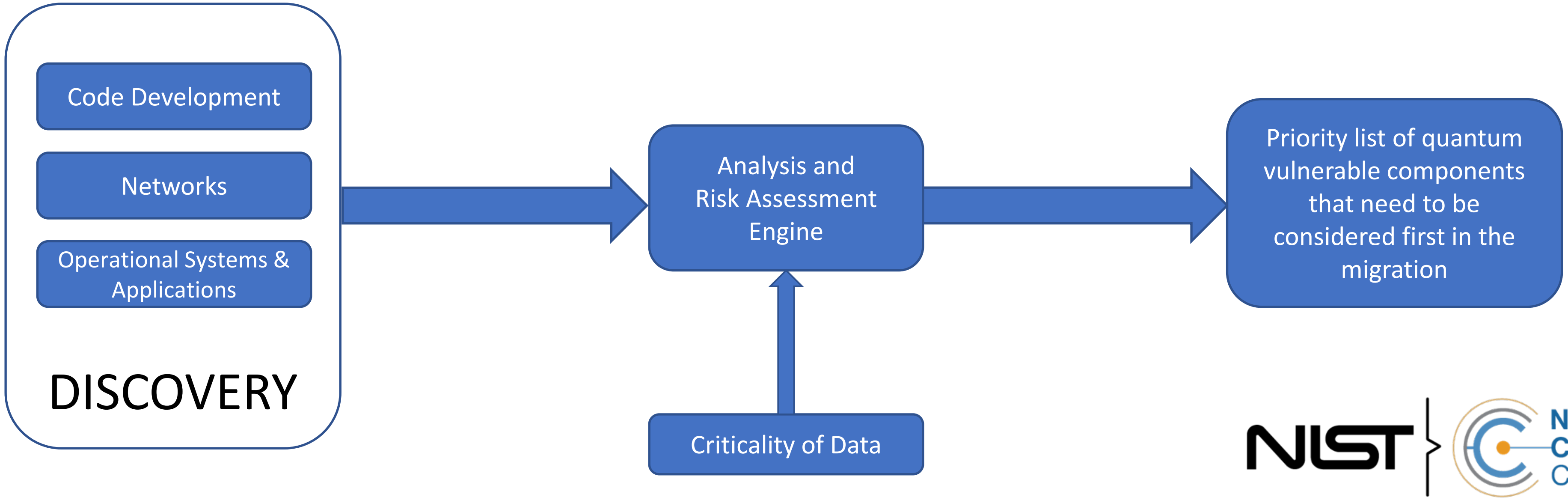
https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

NCCoE Migration to Post-Quantum Cryptography Project Workstreams

Workstream Name	Description
Quantum Vulnerable Algorithm Discovery	• Use discovery tools to detect and report the presence and use of quantum vulnerable cryptography with enough detail and context to inform risk analysis and remediation. • Standardize output formats
Interoperability	• Identifying the challenging problems and bottlenecks that one will face when implementing the first algorithms NIST will standardize as a result of the PQC Standardization Process in protocols such as TLS, SSH, MQTT, QUIC, and a standard like X.509.
Performance	• Identify • Metrics to measure (time, memory); • Protocols to test (e.g., TLS, SSH) and arch/devices to use; • Test conditions (network quality, deployment architectures) • For each test case, and for each implementing software component, measure performance of classical, PQC, and PQ-hybrid cases • Report on unique issues introduced by PQC algorithms • Propose and test solutions to the issues
Outreach / Standards	• Community Outreach
Lab Infrastructure	• Systems, services, and platforms to support technical builds

Discovery Workstream

Workstream Name	Description
Quantum Vulnerable Algorithm Discovery	• **Development Pipeline** - inspects code to find references to cryptography uses that are PQ vulnerable. • **Networks** - Network traffic PQ-vulnerable discovery • **Operational Systems and Applications** - Discovery of PQ-vulnerable applications and libraries at OS-level or provided by the OS itself. • **Risk Analysis** – Development, Network, and Operational Systems discovery informs risk assessment / identification of priorities for replacement


Code Development
Networks
Operational Systems & Applications
DISCOVERY
Analysis and Risk Assessment Engine
Criticality of Data
Priority list of quantum vulnerable components that need to be considered first in the migration

Cryptography Project Team

- **Project Leads & Points of Contact**
  - Bill Newhouse (william.newhouse@nist.gov)
  - Murugiah Souppaya (murugiah.souppaya@nist.gov)
- **Subject Matter Experts**
  - Curt Barker (william.barker@nist.gov)
  - Dustin Moody (dustin.moody@nist.gov)
  - Lily Chen (lily.chen@nist.gov)
- **Lab Task Lead**
  - Chris Brown (christopher.j.brown@nist.gov)
- **Outreach & Engagement**
  - Daniel Eliot (daniel.eliot@nist.gov)

- **Cooperative Research & Development Agreement Consortium Members:**
  - Amazon Web Services, Inc. (AWS)
  - Cisco Systems, Inc.
  - Crypto4A Technologies, Inc.
  - CryptoNext Security
  - Dell Technologies
  - DigiCert
  - IBM
  - InfoSec Global
  - ISARA Corporation
  - JPMorgan Chase Bank, N.A.
  - Microsoft
  - Samsung SDS Co., Ltd.
  - SandboxAQ
  - Thales DIS CPL USA, Inc.
  - Thales Trusted Cyber Technologies
  - VMware, Inc.
  - wolfSSL

Migration to PQC Assumptions & Challenges
Project Drivers

Once an enterprise has discovered where and for what it is employing public-key cryptography, the organization can determine the use characteristics, such as:

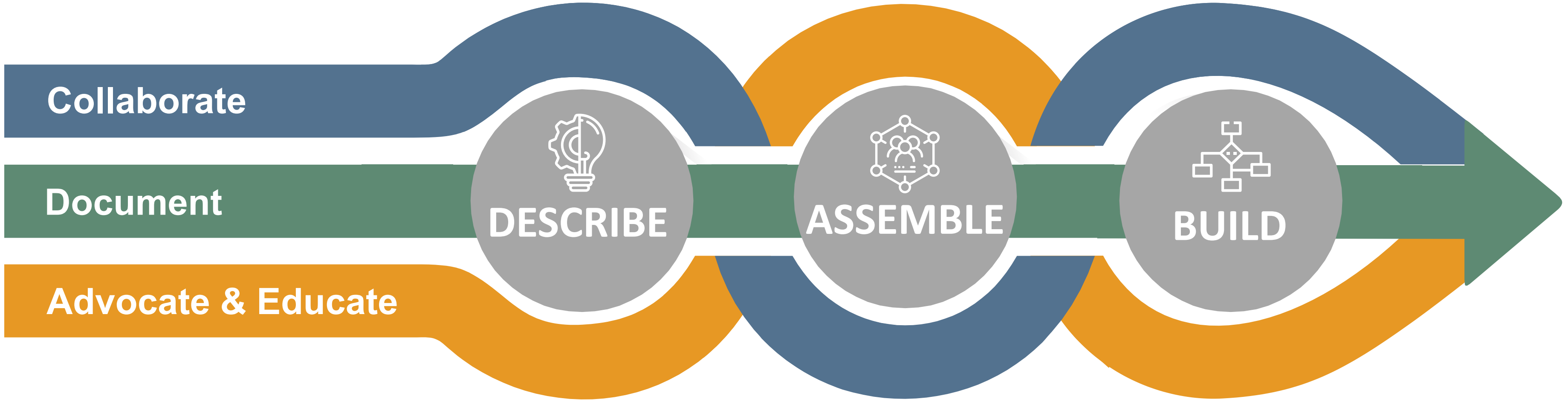
- Current key sizes and hardware/software limits on future key sizes and signature sizes
- Latency and throughput thresholds
- Processes and protocols used for crypto negotiation
- Current key establishment handshake protocols
- Where each cryptographic process is taking place in the stack
- How each cryptographic process is invoked (e.g., by a call to a crypto library, using a process embedded in the operating system, by calling to an application, using cryptography as a service)
- Whether the implementation supports the notion of crypto agility
- Whether the implementation may be updated through software
- Supplier(s) and owner(s) of each cryptographic hardware/software/process
- Source(s) of keys and certificates
- Contractual and legal conditions imposed by and on the supplier
- Whether the use of the implementation requires validation under the Cryptographic Module Validation Program
- The support lifetime or expected end-of-life of the implementation, if stated by the vendor
- Intellectual property impacts of the migration
- Sensitivity of the information that is being protected

Migration to PQC Assumptions & Challenges Project Drivers

Once the replacement algorithms are selected, other operational considerations to accelerate adoption and implementation across the organization include:

- Developing a risk-based approach that takes into consideration security requirements, business operations, and mission impact
- Developing implementation validation tools
- Identifying cases where interim (e.g., hybrid) implementations are necessary to maintaining interoperability during migration.
- Updating the processes and procedures of developers, implementers, and users
- Establishing a communication plan to be used both within the organization and with external customers and partners
- Identifying a migration timeline and the necessary resources
- Updating or replacing security standards, procedures, and recommended practice documentation
- Specifying procurement requirements to acquire quantum-safe technology
- Providing installation, configuration, and administration documentation
- Testing and validating the new processes and procedures

VISUALIZATION OF NCCOE PROJECTS



Practical Migration to Post-Quantum Cryptography Guidance

Define Project Goals

Assemble Team

Build and Demonstrate

Questions

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

applied-crypto-pqc@nist.gov

Project URL:

https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

nccoe.nist.gov

@NISTcyber